



Generating a Key Pair and CSR for a Stronghold Server

Stronghold keys and certificates are managed through three scripts: `genkey`, `getca` and `genreq`. These are part of the normal Stronghold distribution. Keys and certificates are stored in the directory `$SSLTOP/private/`, where `SSLTOP` is typically `/usr/local/ssl`.

To generate a key pair and CSR for your server:

Run `genkey`, specifying the name of the host or virtual host: `genkey hostname`. The `genkey` script displays the filenames and locations of the key file and CSR file it will generate: key file: `/usr/local/www/sslhostname.key` CSR file: `/usr/local/www/sslhostname.cert`

Note: If you already have a key for your server, run `genreq [servername]` to generate only the CSR.

- Press Enter. The `genkey` script reminds you to be sure you are not overwriting an existing key pair and certificate.
- When prompted, enter a key size. Comodo recommends using a 1024 key size.
- When prompted, enter random key strokes. Stop when the counter reaches zero and `genkey` beeps. This random data is used to create a unique public and private key pair.
- When prompted, enter Y to create the key pair and CSR.
- Enter the two-letter country code for your country. You must use the correct ISO country code, other abbreviations will not be recognised. For example, the correct code for United Kingdom is GB.
- Enter the full name of your state or territory. Please do not abbreviate.
- Enter the name of your city, town, or other locality.
- Enter the name of your organisation. This is the full legal name of the organisation applying for the server certificate.
- Enter the name of your unit within the specified organisation. This is usually the group/department the certificate is for.



- Enter your web site's fully-qualified name. For example, www.mydomain.com. This is known as your site's Common Name. The CSR created will look something like this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIBYDCCATECAQAwYgxCzAJBgNVBAYTAIVTMREwDwYDVQQIEwhWaX  
-----More text-----  
U20CbzA7Ur0YBqrnQdD2PnTv/XpHtAAr+M4oez==  
-----END NEW CERTIFICATE REQUEST-----
```

At this point you should back up your key file and CSR to a secure location. If you lose your private key or forget the password, you will not be able to install your certificate

PKI-Partner AB

Box 459

SE-201 24 Malmö

Sweden

Tel ++46 40 631 28 00

Fax +46 40 97 73 93

www.pkipartner.com

(Östergatan 32, 201 22 Malmö)